Remarks

The Office Action mailed August 24, 2005 has been carefully reviewed and the following remarks have been made in consequence thereof.

Claims 16-22, 24-25, and 27-31 are now pending in this application. Claims 16-20, 24, 25, and 27-31 are rejected. Claims 21 and 22 are objected to. Claims 1-15, 23, and 26 are canceled without prejudice, waiver, or disclaimer. Claims 16, 17, 25, 28, and 30 have been amended. No new matter has been added.

The rejection of Claims 25, 27, and 30-31 under 35 U.S.C §112, first paragraph, is respectfully traversed. Applicants respectfully traverse a statement in the Office Action. The statement states, "[t]he counters is non-resettable. It is well-known in the network security art that circumstances such as system failures and lost of network connection disrupt normal sequencing of shared counters/sequence numbers and thus, subsequent valid messages are still be rejected. Since the claimed shared counters are non-resettable and the disclosure fails to teach any procedure to reset or resynchronize the shared counters/sequence numbers in such situations, the disclosure fails to enable one skilled in the art to make and use the claimed invention." Although the Office Action suggests that there is no mention in the specification of any procedure to reset or resynchronize the shared counters/sequence numbers rendering Claims 25, 27, and 30-31 as containing subject matter which is not described in a way to enable one skilled in the art to make and/or use the invention, Applicants respectfully submit that Claims 25, 27, and 30-31 satisfy Section 112, first paragraph. Applicants respectfully submit that one skilled in the art, after reading the specification in light of the figures, would be able to make and/or use the invention as described in Claims 25, 27, and 30-31. Specifically, as an example, the specification states, "In operation, the appliance communication center 510 preferably sends messages forming a reduced message set protocol (RMSP)...to the home appliances 540, 545, 550. The reduced message set protocol (RMSP) is a relatively small library of messages that provide query, command, and information messages between the appliance communication center 510 and

the home appliances...Examples of query messages include "what is your counter setting?", "what is the next counter setting you expect the appliance communication center 510 to use?...Examples of the query response messages include "my counter setting is x"..."the next counter setting I expect the appliance communication center 510 to use is y"...After sending a message requiring authentication to an ECD, the appliance communication center 510 may query the ECD for the next counter setting that the ECD expected the appliance communication center 510 to use. If the shared counter has not been incremented, then the appliance communication center 510 may ask for a copy of the last message that the ECD had expected." (specification, page 17, lines 9-16, page 18, lines 4-10, page 19, lines 2-7, page 26, line 20 – page 27, line 3). Accordingly, the specification provides an example of querying for a counter setting of an appliance and an example of querying for a next counter setting that is expected to be used by the appliance communication center. The examples describe queries to keep a check on values of shared counters between an appliance and the appliance communication center. Moreover, the values of the shared counters can be adjusted by incrementing the values. Hence, as an example, the shared counters can be synchronized by checking the values and incrementing the shared counters. Accordingly, Applicants respectfully requests that the rejection of Claims 25, 27, and 30-31 under Section 112, first paragraph, be withdrawn.

For the reasons set forth above, Applicant respectfully requests that the rejection of Claims 25, 27, and 30-31 under Section 112, first paragraph, be withdrawn.

The rejection of Claims 16-19, 24, and 28-29 under 35 U.S.C. § 103(a) as being unpatentable over Sharrow (U.S. Patent No. 6,061,668) in view of Elgamal et al. (U.S. Patent 5,825,890) and Hoffman et al. (U.S. Patent No. 6,366,682) is respectfully traversed.

Sharrow describes a central management computer (10) that uses a data format to transmit instructions, acknowledgments, and messages to appliances and machines on a network (column 3, lines 12-16). The central management computer checks for an acknowledgment for each transmission sent, and sends an acknowledgment for every data

transmission correctly received (column 3, lines 23-26). The data format used by the central management computer to transmit includes a data field, a message, and a checksum to protect data integrity (column 3, lines 12-16, 20-22).

Elgamal et al. describe a client that delivers a master key to a server in a client-master-key message (column 7, lines 41-42). The master key, for example, can be a randomly generated number (column 7, lines 42-43). The master key is used by the client and the server to produce session keys which will be employed to actually encrypt/decrypt the data to be transferred through a sockets connection (column 7, lines 43-46). The master key is a shared secret between the client and the server (column 7, lines 46-47). The master key is delivered by the client to the server in encrypted form using a key exchange encryption algorithm (column 7, lines 47-49).

Hoffman et al. describe a way to thwart resubmission attacks completely that uses only one sequence number module (SNM) validate packets (column 30, lines 31-32). Under this scheme, there is no update transmission delay window to exploit with a resubmission attack (column 30, lines 32-34). Alternately, multiple SNMs can be active at the same time provided none of them handle sequence number validation for the same biometric input apparatus (BIA)-equipped device (column 30, lines 34-37).

Claim 16 recites in an appliance communication network, a method for authenticating appliance messages, the method comprising "maintaining at an appliance communication center a first shared message counter that counts messages communicated between the appliance communication center and a first appliance, the first shared message counter shared between the communication center and the first appliance; maintaining at the appliance communication center a second shared message counter that counts messages communicated between the appliance communication center and a second appliance, the second shared message counter provides a count separate from a count provided by the first shared message counter; generating a first authentication word by applying an appliance message and the first shared message counter, as stored in the communication center, to an authentication

algorithm; transmitting the appliance message and the first authentication word as an authenticated message to the first appliance; and changing, within the first appliance, a first keying variable by installing a master keying variable within the first appliance and the appliance communication center, wherein the first keying variable is used to generate a second authentication word configured to be compared with the first authentication word, and the second authentication word is different from the appliance message."

None of Sharrow, Elgamal et al., and Hoffman et al., considered alone or in combination, describe or suggest a method for authenticating appliance messages as recited in Claim 16. Specifically, none of Sharrow, Elgamal et al., and Hoffman et al., considered alone or in combination, describe or suggest changing, within the first appliance, a first keying variable by installing a master keying variable within the first appliance and the appliance communication center, where the first keying variable is used to generate a second authentication word configured to be compared with the first authentication word, and the second authentication word is different from the appliance message. Rather, Sharrow describes transmitting by using a data format including a data field, a message, and a checksum, checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal et al. describe delivering a master key to a server in a client-master-key message, producing session keys by using the master key, employing the session keys to encrypt/decrypt the data to be transferred through a sockets connection, and delivering the master key from the client to the server in an encrypted form. Hoffman et al. describe activating multiple sequence number modules (SNMs) at the same time provided none of them handle sequence number validation for the same Biometric Input Apparatus (BIA)-equipped device. Accordingly, none of Sharrow, Elgamal et al., and Hoffman et al., considered alone or in combination, describe or suggest changing, within the first appliance, a first keying variable by installing a master keying variable, where the first keying variable is used to generate a second authentication word configured to be compared with the first authentication word, and the second authentication

word is different from the appliance message. For the reasons set forth above, Claim 16 is submitted to be patentable over Sharrow in view of Elgamal et al. and Hoffman et al.

Claims 17-19 and 24 depend, directly or indirectly, from independent Claim 16. When the recitations of Claims 17-19 and 24 are considered in combination with the recitations of Claim 16, Applicants submit that dependent Claims 17-19 and 24 likewise are patentable over Sharrow in view of Elgamal et al. and Hoffman et al.

Claim 28 recites a system comprising "a first appliance including: a first shared message counter; a processor; and a memory coupled to the processor, the memory storing instructions for execution by the processor for: receiving an authenticated message, including a first authentication word and an appliance message, at the first appliance; generating a second authentication word by applying the first shared message counter, as stored in the first appliance, and the appliance message to an authentication algorithm; and comparing the first authentication word and the second authentication word to determine authenticity of the authenticated message; a second appliance separate from the first appliance; and an appliance communication center including a second shared message counter and a third shared message counter, the second shared message counter shared between the appliance communication center and the first appliance, the third shared message counter shared between the communication center and the second appliance, and the third shared message counter configured to provide a count separate from a count provided by the second shared message counter, wherein the memory configured to store instructions to change, within the first appliance, a first keying variable by installing a master keying variable within the first appliance and the appliance communication center, wherein the first keying variable is used to generate the second authentication word."

None of Sharrow, Elgamal et al., and Hoffman et al., considered alone or in combination, describe or suggest a system as recited in Claim 28. Specifically, none of Sharrow, Elgamal et al., and Hoffman et al., considered alone or in combination, describe or suggest the memory configured to store instructions to change, within the first appliance, a

first keying variable by installing a master keying variable within the first appliance and the appliance communication center, where the first keying variable is used to generate the second authentication word. Rather, Sharrow describes transmitting by using a data format including a data field, a message, and a checksum, checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal et al. describe delivering a master key to a server in a client-master-key message, producing session keys by using the master key, employing the session keys to encrypt/decrypt the data to be transferred through a sockets connection, and delivering the master key from the client to the server in an encrypted form. Hoffman et al. describe activating multiple sequence number modules (SNMs) at the same time provided none of them handle sequence number validation for the same Biometric Input Apparatus (BIA)-equipped device. Accordingly, none of Sharrow, Elgamal et al., and Hoffman et al., considered alone or in combination, describe or suggest the memory configured to store instructions to change, within the first appliance, a first keying variable by installing a master keying variable, where the first keying variable is used to generate the second authentication word. For the reasons set forth above, Claim 28 is submitted to be patentable over Sharrow in view of Elgamal et al. and Hoffman et al.

Claim 29 depends from independent Claim 28. When the recitations of Claim 29 are considered in combination with the recitations of Claim 28, Applicants submit that dependent Claim 29 likewise is patentable over Sharrow in view of Elgamal et al. and Hoffman et al.

For at least the reasons set forth above, Applicants respectfully request that the rejection of Claims 16-19, 24, and 28-29 under 35 U.S.C. 103(a) be withdrawn.

The rejection of Claims 25, 27, and 30-31 under 35 U.S.C. § 103(a) as being unpatentable over Sharrow in view of Elgamal et al., Hoffman et al., and "Commercial Laundry Services", available at http://www.cinetworks.com/~jetz/comrcl.html, is respectfully traversed.

Sharrow, Elgamal et al., Hoffman et al. are described above.

Commercial Laundry Services describes a JETZ equipment that includes a temper-resistant vault. The JETZ equipment also includes a non-resettable counter which insures accountability.

Claim 25 recites a system comprising "a plurality of appliances including a first appliance and a second appliance; and an appliance communication center including: network connections terminating at the appliances; a processing circuit; a memory storing a plurality of shared counters including a first shared message counter and a second shared message counter, the first shared message counter shared between the appliance communication center and the first appliance, the second shared message counter shared between the communication center and the second appliance, the first shared message counter configured to provide a count separate from a count provided by the second shared message counter, the first and second shared message counters configured to be non-resettable, the memory further storing instructions for: maintaining at the appliance communication center the first shared message counter; generating a first authentication word by applying an appliance message and the first shared message counter, as stored in the appliance communication center, to an authentication algorithm; transmitting the appliance message and the first authentication word as an authenticated message to the first appliance; and transmitting a command to change, within the first appliance, a first keying variable, wherein the first keying variable is changed by installing a master keying variable within the first appliance and the appliance communication center, and the first keying variable is used to generate a second authentication word configured to be compared with the first authentication word."

None of Sharrow, Elgamal et al., Hoffman et al., and Commercial Laundry Services, considered alone or in combination, describe or suggest a system as recited in Claim 25. Specifically, none of Sharrow, Elgamal et al., Hoffman et al., and Commercial Laundry Services, considered alone or in combination, describe or suggest the memory further storing instructions for transmitting a command to change, within the first appliance, a first keying

variable, where the first keying variable is changed by installing a master keying variable within the first appliance and the appliance communication center, and the first keying variable is used to generate a second authentication word configured to be compared with the first authentication word. Rather, Sharrow describes transmitting by using a data format including a data field, a message, and a checksum, checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal et al. describe delivering a master key to a server in a client-master-key message, producing session keys by using the master key, employing the session keys to encrypt/decrypt the data to be transferred through a sockets connection, and delivering the master key from the client to the server in an encrypted form. Hoffman et al. describe activating multiple sequence number modules (SNMs) at the same time provided none of them handle sequence number validation for the same Biometric Input Apparatus (BIA)-equipped device. Commercial Laundry Services describes insuring accountability by using a non-resettable counter. Accordingly, none of Sharrow, Elgamal et al., Hoffman et al., and Commercial Laundry Services, considered alone or in combination, describe or suggest the memory further storing instructions for transmitting a command to change, within the first appliance, a first keying variable, where the first keying variable is changed by installing a master keying variable, and the first keying variable is used to generate a second authentication word configured to be compared with the first authentication word. For the reasons set forth above, Claim 25 is submitted to be patentable over Sharrow in view of Elgamal et al. Hoffman et al., and Commercial Laundry Services.

Claim 27 depends from independent Claim 25. When the recitations of Claim 27 are considered in combination with the recitations of Claim 25, Applicants submit that dependent Claim 27 likewise is patentable over Sharrow in view of Elgamal et al. Hoffman et al., and Commercial Laundry Services.

Claim 30 recites in an appliance communication network, a method for authenticating appliance messages, the method comprising "maintaining at a first appliance a first non-

resettable shared message counter, the first non-resettable shared message counter shared between the first appliance and a remotely located appliance communication center; maintaining at the appliance communication center a second non-resettable shared message counter that counts messages communicated between the appliance communication center and the first appliance; maintaining at the appliance communication center a third non-resettable shared message counter that counts messages communicated between the appliance communication center and a second appliance, the third non-resettable shared message counter provides a count separate from a count provided by the second non-resettable shared message counter; generating a first authentication word by applying an appliance message and the first non-resettable shared message counter, as stored in the first appliance, to an authentication algorithm; transmitting the appliance message and the first authentication word as an authenticated message to the appliance communication center; and changing, within the first appliance, a first keying variable by installing a master keying variable within the first appliance and the appliance communication center, wherein the first keying variable is used to generate the first authentication word."

None of Sharrow, Elgamal et al., Hoffman et al., and Commercial Laundry Services, considered alone or in combination, describe or suggest a method for authenticating appliance messages as recited in Claim 30. Specifically, none of Sharrow, Elgamal et al., Hoffman et al., and Commercial Laundry Services, considered alone or in combination, describe or suggest changing, within the first appliance, a first keying variable by installing a master keying variable within the first appliance and the appliance communication center, where the first keying variable is used to generate the first authentication word. Rather, Sharrow describes transmitting by using a data format including a data field, a message, and a checksum, checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal et al. describe delivering a master key to a server in a client-master-key message, producing session keys by using the master key, employing the session keys to encrypt/decrypt the data to be transferred through a sockets connection, and delivering the master key from the client to the server in an

encrypted form. Hoffman et al. describe activating multiple sequence number modules (SNMs) at the same time provided none of them handle sequence number validation for the same Biometric Input Apparatus (BIA)-equipped device. Commercial Laundry Services describes insuring accountability by using a non-resettable counter. Accordingly, none of Sharrow, Elgamal et al., Hoffman et al., and Commercial Laundry Services, considered alone or in combination, describe or suggest changing, within the first appliance, a first keying variable by installing a master keying variable, where the first keying variable is used to generate the first authentication word. For the reasons set forth above, Claim 30 is submitted to be patentable over Sharrow in view of Elgamal et al. Hoffman et al., and Commercial Laundry Services.

Claim 31 depends from independent Claim 30. When the recitations of Claim 31 are considered in combination with the recitations of Claim 30, Applicants submit that dependent Claim 31 likewise is patentable over Sharrow in view of Elgamal et al. Hoffman et al., and Commercial Laundry Services.

For at least the reasons set forth above, Applicants respectfully request that the rejection of Claims 25, 27, and 30-31 under 35 U.S.C. 103(a) be withdrawn.

The rejection of Claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Sharrow in view of Elgamal et al., Hoffman et al., and further in view of Kaufman et al. (*Network Security: Private Communication in a Public World*), is respectfully traversed.

Sharrow, Elgamal et al., and Hoffman et al. are described above.

Kaufman et al. describe a system that avoids an implausible attack (page 242, third paragraph). The system avoids the attack by using sequence numbers in different ranges for two directions, by having a DIRECTION BIT somewhere in a message, or by having an integrity code computed by some subtly different algorithm in the two directions (page 242, third paragraph).

Claim 20 depends indirectly from Claim 16 which recites in an appliance communication network, a method for authenticating appliance messages, the method comprising "maintaining at an appliance communication center a first shared message counter that counts messages communicated between the appliance communication center and a first appliance, the first shared message counter shared between the communication center and ~~a~~the first appliance; maintaining at the appliance communication center a second shared message counter that counts messages communicated between the appliance communication center and a second appliance, the second shared message counter provides a count separate from a count provided by the first shared message counter; generating a first authentication word by applying an appliance message and the first shared message counter, as stored in the communication center, to an authentication algorithm; transmitting the appliance message and the first authentication word as an authenticated message to the first appliance; and changing, within the first appliance, a first keying variable by installing a master keying variable within the first appliance and the appliance communication center, wherein the first keying variable is used to generate a second authentication word configured to be compared with the first authentication word, and the second authentication word is different from the appliance message."

None of Sharrow, Elgamal et al., Hoffman et al., and Kaufman et al., considered alone or in combination, describe or suggest a method for authenticating appliance messages as recited in Claim 16. Specifically, none of Sharrow, Elgamal et al., Hoffman et al., and Kaufman et al., considered alone or in combination, describe or suggest changing, within the first appliance, a first keying variable by installing a master keying variable within the first appliance and the appliance communication center, where the first keying variable is used to generate a second authentication word configured to be compared with the first authentication word, and the second authentication word is different from the appliance message. Rather, Sharrow describes transmitting by using a data format including a data field, a message, and a checksum, checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal et al. describe

delivering a master key to a server in a client-master-key message, producing session keys by using the master key, employing the session keys to encrypt/decrypt the data to be transferred through a sockets connection, and delivering the master key from the client to the server in an encrypted form. Hoffman et al. describe activating multiple sequence number modules (SNMs) at the same time provided none of them handle sequence number validation for the same Biometric Input Apparatus (BIA)-equipped device. Kaufman et al. describe using a plurality of sequence numbers in different ranges for two directions, having a DIRECTION BIT somewhere in a message, or having an integrity code computed by some subtly different algorithm in the two directions. Accordingly, none of Sharrow, Elgamal et al., Hoffman et al., and Kaufman et al., considered alone or in combination, describe or suggest changing, within the first appliance, a first keying variable by installing a master keying variable, where the first keying variable is used to generate a second authentication word configured to be compared with the first authentication word, and the second authentication word is different from the appliance message. For the reasons set forth above, Claim 16 is submitted to be patentable over Sharrow in view of Elgamal et al., Hoffman et al., and further in view of Kaufman et al.

When the recitations of Claim 20 are considered in combination with the recitations of Claim 16, Applicants submit that dependent Claim 20 likewise is patentable over Sharrow in view of Elgamal et al., Hoffman et al., and further in view of Kaufman et al.

For at least the reasons set forth above, Applicants respectfully request that the rejection of Claim 20 under 35 U.S.C. 103(a) be withdrawn

Moreover, Applicants respectfully submit that the 35 U.S.C. § 103 rejections of Claims 16-20, 24, 25, and 27-31 are not proper rejections. As is well established, obviousness cannot be established by combining the teachings of the cited art to produce the claimed invention, absent some teaching, suggestion, or incentive supporting the combination. None of Sharrow, Elgamal et al., Hoffman et al., Commercial Laundry Services, or Kaufman et al., considered alone or in combination, describe or suggest the

claimed combination. Furthermore, in contrast to the assertion within the Office Action, Applicants respectfully submit that it would not be obvious to one skilled in the art to combine Sharrow with Elgamal et al., Hoffman et al., Commercial Laundry Services, or Kaufman et al. because there is no motivation to combine the references suggested in the art.

As the Federal Circuit has recognized, obviousness is not established merely by combining references having different individual elements of pending claims. Ex parte Levengood, 28 U.S.P.Q.2d 1300 (Bd. Pat. App. & Inter. 1993). MPEP §2143.01. Rather, there must be some suggestion, outside of Applicants' disclosure, in the prior art to combine such references, and a reasonable expectation of success must be both found in the prior art, and not based on Applicants' disclosure. In re Vaeck, 20 U.S.P.Q.2d 1436 (Fed. Cir. 1991). In the present case, neither a suggestion or motivation to combine the prior art disclosures, nor any reasonable expectation of success has been shown.

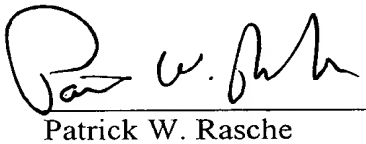
Furthermore, it is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the cited art so that the claimed invention is rendered obvious. Specifically, one cannot use hindsight reconstruction to pick and choose among isolated disclosures in the art to deprecate the claimed invention. Further, it is impermissible to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. The present 35 U.S.C. § 103 rejections are based on a combination of teachings selected from multiple patents in an attempt to arrive at the claimed invention. Specifically, Sharrow teaches transmitting by using a data format including a data field, a message, and a checksum, checking for an acknowledgment for each transmission sent and sending an acknowledgment for every data transmission correctly received. Elgamal et al. teach delivering a master key to a server in a client-master-key message, producing session keys by using the master key, employing the session keys to encrypt/decrypt the data to be transferred through a sockets connection, and delivering the master key from the client to the server in an encrypted form. Hoffman et al.

teach activating multiple sequence number modules (SNMs) at the same time provided none of them handle sequence number validation for the same Biometric Input Apparatus (BIA)-equipped device. Commercial Laundry Services teaches insuring accountability by using a non-resettable counter. Kaufman et al. teach using a plurality of sequence numbers in different ranges for two directions, having a DIRECTION BIT somewhere in a message, or having an integrity code computed by some subtly different algorithm in the two directions. Otherwise, there is a possibility of running out of the sequence numbers during the conversation. Because there is no teaching nor suggestion in the cited art for the combination, the 35 U.S.C. § 103 rejections appear to be based on a hindsight reconstruction in which isolated disclosures have been picked and chosen in an attempt to reject the claims of the present application. Of course, such a combination is impermissible, and for this reason Applicants request that the 35 U.S.C. § 103 rejections of Claims 16-20, 24, 25, and 27-31 be withdrawn.

For at least the reasons set forth above, Applicants respectfully request that the 35 U.S.C. § 103 rejections of Claims 16-20, 24, 25, and 27-31 be withdrawn.

In view of the foregoing remarks, this application is believed to be in condition for allowance. Reconsideration and favorable action is respectfully solicited.

Respectfully Submitted,



Patrick W. Rasche
Registration No. 37,916
ARMSTRONG TEASDALE LLP
One Metropolitan Square, Suite 2600
St. Louis, Missouri 63102-2740
(314) 621-5070